Evaluasi kinerja chaotic, advanced dan data encryption standard pada aliran data UDP dalam jaringan simulasi NS3 point-to-point yang tidak bebas kesalahan = Comparison of chaotic, advanced and data encryption standard on UDP data stream in a non error free NS3 simulated point-to-point network

Elvian Syafrurizal, author

Abstrak

Dalam komunikasi data, dengan meningkatnya jumlah dan keparahan serangan ancaman cyber harian, enkripsi menjadi salah satu alat penting untuk memastikan keamanan data dalam perjalanan. Meskipun AES, terutama AES-256, saat ini dianggap sebagai penerus DES yang dapat memberikan keamanan tersebut, itu tidak akan tetap menjadi status quo. Dengan kemajuan penelitian komputasi kuantum, keamanan yang diberikan oleh AES tidak akan bertahan lama. Dengan demikian, penelitian untuk enkripsi berbasis chaotic map, Chaotic Encryption Standard (CES) pada akhirnya akan menjadi kandidat prospektif untuk penerus AES. Namun demikian, metode enkripsi seperti CES tidak hanya perlu tahan terhadap upaya cracking, tetapi juga harus mempertahankan informasi yang tersimpan di dalamnya saat sedang ditransfer. Dalam percobaan ini, aliran data yang dienkripsi dalam CES, dalam hal ini CES (PCMPB/K), dibandingkan dengan yang dienkripsi dalam AES-256 dan DES. Semua dijalankan melalui simulasi NS3 dengan jaringan tidak bebas-kesalahan menggunakan UDP sebagai enkapsulasi paket. Hasil percobaan menunjukkan bahwa meskipun CES (PCMPB/K) memang lebih sulit untuk di rusak daripada AES256 dan DES, hal tersebut itu menimbulkan risiko yang lebih tinggi untuk tidak dapat dibaca dalam jaringan tidak bebas-kesalahan karena ukuran bit blok besar yaitu 16 kali dari AES-256 dan 32 kali DES.
.....In data communication, with increasing number and severity of day to day cyber-threat attacks, encryption becomes one of the crucial tools to ensure the security of data in transit. Although AES, especially AES-256, currently considered as the successor of DES that can give such security, it will not remain a status quo. With the advancements of quantum computing research, the security provided by AES is not going to stand for long. Thus, the research for chaotic map-based encryption, Chaotic Encryption Standard (CES) will eventually become prospective candidate for AES successor. Nevertheless, encryption method like CES not only needs to be resistant to cracking effort, but it also has to retain the information held within while being transferred. In this experiment, streams of data encrypted in CES, in this case CES(PMCS/E), is compared to the ones encrypted in AES-256 and DES. All are run through an NS3 simulation with non-error free network using UDP as packet encapsulation. The results of the experiment show that even though CES(PMCS/E) is indeed harder to crack than AES256 and DES, it poses higher risk to be unreadable in a non-error free network due to the large block bit size which is 16 times of the AES-256 and 32 times of the DES.